IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

IN THE MATTER OF THE SEARCH OF: 19 W Gregson Avenue #207, South Salt Lake Utah 84115	Case No. 2:23m668-DAO_____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michael Phillips, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigator and sworn law enforcement officer for the State of Utah. I am currently an agent with the Utah State Bureau of Investigation. I am a Task Force Officer with the Federal Bureau of Investigation (FBI) currently assigned to the FBI Public Corruption Task Force in the Salt Lake City, Utah. The information contained in this complaint is based on an investigation conducted by your affiant along with Federal Bureau of Investigation TFO (task force officer) agents from the Utah Department of Public Safety State Bureau of Investigation and other law enforcement officers.
2. This affidavit is submitted in support of applications for a Search Warrant for a residence located at 19 W Gregson Avenue #207, South Salt Lake Utah 84115 for

evidence related to the violation of Title 18 United States Code Section 875(c), Interstate communications/ Threatening Communications

3. Facts in this affidavit come from information obtained from other agent's, law enforcement officers, and witnesses. Your affiant has read and become familiar with the facts set forth in this affidavit. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

FACTS ESTABLISHING PROBABLE CAUSE

4. On July 11, 2023, the Utah Film Commission (film@utah.gov) received an email from Philip Johnson using the email address anillegitimategov@gmail.com. The subject line of the email read: "MOVE LIKE YOUR LIFE DEPENDS ON IT!"

5. In the last paragraph of the email, Johnson stated, "By the way I have sent a demand for individual combat to the office of the Governor of Utah for past to current offenses. I intend to kill the little dude on the 25th at about noon for having perpetuated them. I'm sure you'll find the detestable little man is as entirely dispensable as the regrettable of forgettable string of them to date." The "little dude" referenced in the email has been identified as Governor Cox, State of Utah. In prior communications Johnson has expressed displeasure with the Governor and the Governor's Office. The communication was forwarded to the Utah State Bureau of Investigation Threat Management Unit for investigation.

6. Philip Johnson has for at least the last 5 years demanded from the Utah Film Commission a detailed list of all "film locations" in the State of Utah dating back to 1966. In August of 2018 Johnson sent threatening emails, which were read by the Utah State Capital Constituent Services, the emails were reported to the Utah Highway Patrol Executive Protection supervisor Sgt. G. Hansen. Utah State Bureau of Investigation Agents responded to Johnson's home to conduct an interview of Johnson. Johnson stated, "No warrant, no access" and closed the door.

7. Johnson suffered from a period of homelessness and was assigned a case worker. Contact was made with the case worker and she was asked to make contact with Johnson. The case worker made contact with Johnson. According to Johnson's case worker, when asked about the threats, Johnson stated, "the police can go fuck themselves."

8. On July 13, 2023, your Affiant and other Agents with the Utah State Bureau of Investigation attempted to make contact with Johnson at 19 West Gregson #207, regarding the most recent threatening email as described above. Johnson opened the door, the SBI Agent introduced himself and asked Johnson if he would be able to answer a few questions. Johnson stated, "screw off, ciao" and closed the door thus confirming the place of residence of Philips S. Johnson.

9. On July 14, 2023, exigent subscriber requests were sent to Google for the email address anillegitimategov@gmail.com. Google responded and gave an IP address: 75.169.10.104, with a recovery SMS of (801) 580-2117. The email address anillegitimategov@gmail.com is registered to Philip Johnson. The number (801) 580-2117 is a documented and current contact phone number for Philip Johnson residing at 19 West Gregson Avenue #207 in South Salt Lake City, Utah 84115.
10. Law Enforcement database searches were conducted and confirmed Philip Johnson with the date of birth of 11-13-1966 currently resides at 19 West Gregson Avenue #207 in South Salt Lake City, UT 84115.
11. On 7/17/2023 Johnson was observed entering and leaving 19 West Gregson Avenue in South Salt Lake City. Johnson was observed exiting and entering his apartment building. Johnson was alone when he both enters and leaves the residence. He was on foot and believed to not have any other means of transportation other than by foot and public transportation. I confirmed from Grace Mary Manor that Philip Johnson is the sole occupant of apartment #207.
12. On 7/17/2023 a complaint was obtained for the arrest of Philip Johnson for violation of Title 18 United States Code Section 875(c), Interstate communications/ Threatening Communications, Case No. 2:23mj657-DAO. Johnson was taken in custody without incident. During a search incident to arrest a thumb drive was seized from Johnson's person and booked into evidence.

13. I know from my training and experience that subjects who have made threats through email and electronic means typically have evidence pertaining to those crimes in their residence. This evidence typically includes computers, hard drives storage devices, cellular phones, data storage devices including USB and SD cards, cameras and recording devices, writings/ documents, photographs/ images, which can contain evidence of the crime.

14. Based on the facts and circumstances described herein, I submit there is probable cause to believe there is evidence related to the above crime located at 19 West Gregson Avenue #207 in South Salt Lake City, UT 84115.

TECHNICAL TERMS

15. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses,

while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

16. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

17. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of

how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of

information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions

about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

19. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage

media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

21. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Michael Phillips

Michael Phillips
Special Agent/FBI TFO
Utah Department of Public Safety
State Bureau of Investigation
Threat Management Unit

Subscribed and sworn to before me
on July 25, 2023:

Daphne A. Oberg

DAPHNE A. OBERG
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is 19 W Gregson Avenue #207, South Salt Lake Utah 84115, further described as an apartment building.

ATTACHMENT B

1. All records relating to violations of 18 U.S.C. § 875(c), Threatening Communications and involving Philip Johnson since July 11, 2023, including:

a. Email communications from Philip Johnson to the Utah Film Commission, Office of the Governor for the State of Utah;

b. any information recording Philip Johnson's schedule or travel from July 11, 2023 to July 25, 2023, the date of the execution of the threat ;

2. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant.

3. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as

well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of the Internet Protocol address 75.169.10.104 to communicate with Utah Film Commission, Office of the Governor for the State of Utah, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).